

REMARKS

In response to the Office Action mailed on November 2, 2005, Applicants respectfully request reconsideration. To further the prosecution of this Application, Applicants submit the following remarks discussing patentability of rejected and newly added claims. Applicants respectfully request that the application be passed to issue.

Claims 1-32 were previously pending in the subject Application. Claims 33-40 are being added by way of this amendment. Thus, after entry of this Amendment, claims 1-40 will be pending. No new matter was added to the application when amending or adding these claims. Also, the submission of any amendments should not be interpreted as acquiescing to any of the rejections.

The following remarks address the rejections of claims 1-32 as set out in the present Office Action and patentability of newly added claims 33-40. Applicants respectfully request reconsideration. Applicant is appreciative of the Examiner's review of the claims and allowance of claims 12 and 27.

Summary of an Embodiment of the Invention

Prior to discussion of the pending claims, Applicants would like to briefly discuss an illustrative embodiment of the present invention. One embodiment of the present invention, in contrast to conventional approaches, is directed to a technique for authenticating devices in a network such as a Radio Frequency Identification (RFID) Network between control stations and one or more transceivers. A transceiver receives transceiver configuration information including a network address and transceiver authentication credentials and receives an authentication request from the control station. The transceiver applies authentication processing to request information within the authentication request in conjunction with the transceiver authentication credentials to produce an authentication response and transmits the authentication response to the

control station to allow the control station to determine if the transceiver is authorized to communicate within the remote identification system.

Rejections of Claim 1, 13, 16, 28, 31, and 32 under 35 U.S.C. § 102(b)

The Examiner has rejected claim 1 under 35 U.S.C. § 102(b) as being unpatentable over Chan (U.S. Patent 6,128,389). Applicants are appreciative of the Examiner's review of pending claim 1 and respectfully request further consideration.

Applicants respectfully traverse the rejection because Chan does not teach or suggest every claim limitation. For example, Chan does not teach or suggest limitations of "receiving transceiver configuration information including a network address and transceiver authentication credentials, receiving an authentication request from a control station within the remote identification system; applying authentication processing to request information within the authentication request in conjunction with the transceiver authentication credentials to produce an authentication response; and transmitting the authentication response to the control station to allow the control station to determine if the transceiver is authorized to communicate within the remote identification system."

Without providing a specific comparison of the claimed elements and the techniques in Chan, the office action cites the following paragraph in Chan to reject elements of the claimed invention:

"FIG. 11 is an example of a registration signaling process including authentication according to one embodiment of the present invention. In FIG. 11 an MSC/VLR 302A and the SAC 902 in the signaling gateway/SAC system 303 perform an authentication procedure. At time A the MSC/VLR 302A in the IS-41C system transmits an authentication request signal (AUTHREQ) to the gateway/SAC

-20-

system 303 which forwards the request to the SAC 902. The authentication request includes an authentication value based upon a global authentication challenge (GC). The SAC 902 stores an SSD2 value in the MS identification data unit 420. The operation of the SAC 902 is similar to the operation of the SAC 206 described above. The SAC 902 compares the GC value with the value determined based upon the authentication algorithm and the MS information, e.g., the MIN, ESN, and the SSD2 signals. If the GC matches the value determined by the SAC 902, the SAC can identify the MS as authentic or it can challenge the MS to generate another authentication value.” (emphasis added)

Applicant respectfully submits that the techniques in the above passage are not equivalent to what the Applicant claims as the present invention recited in claim 1. According to this passage in Chan, a mobile switching center transmits the authentication request. Applicants assume that the office action likens the mobile switching center generating the request to the control station as recited by the claimed invention. As underlined in the cited passage, Chan further recites that gateway/SAC 303 utilizes SAC to compare a GC value (in the request message) with another value determined based on MS information associated with a respective Mobile Station being authenticated. There is no indication in this portion of the cited passage that the gateway/SAC 303 transmits an authentication response to the mobile switching center (e.g., the element likened to the control station in the claimed invention). This is opposite of the language recited in claim 1. For example, claim 1 recites “in a transceiver,” “receiving an authentication request,” “applying authentication processing to request information within the authentication request,” and “transmitting an authentication response” to the control station. There is no indication in this portion of the cited passage that the gateway/SAC 303 or any other entity in Chan performs these functions. Thus, this portion of the cited passage does not teach or suggest the claimed invention.

The balance of the above cited passage reads as follows and also does not disclose the limitations in the claimed invention:

At time B the SAC 902 issues a response to the authentication signal (authreq[UC]) requesting that the MS generate another authentication value. This response signal includes a "unique challenge" having a random value and the expected response value based upon the effect of the authentication procedure on the random value. The random value is transmitted to the MS 102 which determines a new authentication value using the process described above, for example. The SAC 902 requests an Update/unique challenge request in order to update the value of the SSD in the MS 102 which can be used when whenever the SSD is to be updated. The MSC/VLR 302A compares the new authentication value with the expected response value. The MSC/VLR 302A transmits an authentication report command (ASREPORT[UCRPT]) to the SAC 902 at time C indicating whether the MS 102 has passed or failed the authentication procedure. The SAC 902 acknowledges the message at time D using the authentication report response (asreport). If the MS 102 is authenticated, the MSC/VLR 302A attempts to register the MS 102 at time E by transmitting a registration notification signal (REGNOT) to the signaling gateway/SAC system 303. If the MS 102 satisfied the authentication process, the signaling gateway/SAC system 303 transmits a registration notification command (REGNOT) to the HLR of the home system at time F. If the MS 102 does not satisfy the authentication process the SAC 902 prevents the MS 102 from registering using the technique set forth in a conventional authentication protocol. After receiving the registration notification command (REGNOT), the home system HLR 310B generates and transmits a registration notification response signal (regnot) to the signaling gateway/SAC system 303. The signaling gateway/SAC system 303 then generates and transmits a registration notification response signal (regnot) to the MSC/VLR 302A. This completes the authentication and registration process of an MS 102 transmitting through the MSC/VLR 302A. Accordingly, even though the home system HLR

310B for the MS 102 was not capable of authenticating the MS 102 using the IS-41C authentication procedure, the present invention enables the MS 102 to utilize this feature while visiting a system supporting authentication. In addition, the SAC 902 performs the authentication procedure without having access to sensitive authentication information, e.g., the A-key." (emphasis added)

According to this section of the cited passage in Chan, the SAC 902 in gateway 303 generates the authentication request. Applicants therefore assume that the office action likens the SAC 902 in gateway 303 generating the request to the "control station" as recited by the claimed invention. Recall again that the claimed invention recites, *inter alia*, "receiving an authentication request from a control station," producing an authentication response, and thereafter "transmitting the authentication response to the control station." That is, a first entity (e.g., a transceiver) receives an authentication request from the control station and transmits a reply back to the control station. There is no indication in this portion of the cited passage that the mobile station receives the authentication request from the gateway/SAC 303 and transmits a respective authentication response back to the gateway/SAC 303. Instead, Chan indicates that the mobile station only generates the "new authentication value" and "the MSC/VLR 302A compares the new authentication value with the expected response value." The mobile station in Chan does not transmit the authentication response to the SAC 902 in gateway 303, which was the entity generating the authentication request. Thus, the cited passage does not teach every claim limitation.

Moreover, in addition to the above differences, claim 1 recites that a claimed transceiver herein supports "applying authentication processing to request information within the authentication request in conjunction with the transceiver authentication credentials to produce an authentication response." In other words, authentication processing of the claimed invention is applied to both

information in the authentication request as well as corresponding transceiver authentication credentials previously received by the transceiver. The cited passage only indicates that a respective authentication response (e.g., challenge response) is generated a “unique challenge value” such as a random value received in the authentication request and not information (e.g., transceiver authentication credentials) associated with the entity generating the response.

Based on the aforementioned remarks, Applicant respectfully submits that the invention as recited in claim 1 is neither anticipated nor obvious because it includes a unique and useful configuration not taught or suggested by cited references Chan or any other reference of record. Thus, in view of the foregoing discussion, Applicants submit that claim 1 in its original form is patentably distinct over the cited prior art, and the obviousness rejection should be withdrawn. Claims 2-12 depend from claim 1 and therefore also should be in condition for allowance.

Claims 16 and 31 include similar limitations as claim 1 and should be allowable for similar reasons. Claims 17-27 depend from claim 16 and therefore also should be in condition for allowance.

Claim 13 recites “providing transceiver configuration information including a network address and transceiver authentication credentials to a transceiver; providing an authentication request from the control station within the remote identification system to the transceiver, the authentication request containing a request authentication result and a request data value; receiving an authentication response from the transceiver, the authentication response containing an authentication response answer to the authentication request; and determining if the authentication response answer is valid by applying authentication processing to the authentication response answer within the authentication response in conjunction with the transceiver authentication

credentials, and if the authentication response answer is valid, transmitting an authentication success message to the transceiver.” For similar reasons as discussed above, Applicant respectfully submits that claim 13 is allowable over Chan. For example, claim 13 recites that a first entity (i.e., a control station) provides transceiver configuration information as well as an authentication to a second entity (i.e., a transceiver). The claim further recites receiving an authentication response from the second entity and determining whether the authentication response is valid. As discussed above, this back and forth communication technique is not recited by Chan. Additionally, claim 13 recites applying authentication processing to the authentication response answer within the authentication response in conjunction with the transceiver authentication credentials. Note again that the transceiver authentication credentials were sent to the first entity (e.g., the transceiver) in another step. Chan also does not teach or suggest this claim limitation. Further, Chan does not recite transmitting an authentication success message back the entity that generated the authentication response. More specifically, Chan recites that “The MSC/VLR 302A transmits an authentication report command (ASREPORT[UCRPT]) to the SAC 902 at time C indicating whether the MS 102 has passed or failed the authentication procedure” That is, neither the MSC/VLR nor the SAC 902 sends a confirmation back to the mobile station whether authentication was successful. Claims 14-15 depend from claim 13 and therefore also should be in condition for allowance.

Claims 28 and 32 include similar limitations as claim 13 and should be allowable for similar reasons. Claims 29 and 30 depend from claim 28 and therefore also should be in condition for allowance.

Note that the dependent claims include yet further distinguishing features over the cited prior art and are allowable for additional reasons as well. For example, certain dependent claims recite use of a set of authentication

-25-

instructions and corresponding authentication values in the transceiver. The cited prior art fails to disclose use of such information.

New Claims 33-40

Applicant has added claims 33-40, which further narrow claim 1 over the cited prior art. Support for these claims can be found (among other places) at page 14, line 13 to page 20, line 18 and corresponding figures. Note that claims 33-36 have certain limitations found in objected to claim 12. The other claims are similar to other rejected claims. Applicants respectfully request that the Examiner allow these claims as well the originally pending claims.

CONCLUSION

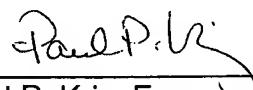
In view of the foregoing remarks, Applicants submit that the pending claims as well as newly added claims are in condition for allowance. A Notice to this affect is respectfully requested. If the Examiner believes, after reviewing this Response, that the pending claims are not in condition for allowance, the Examiner is respectfully requested to call the Applicant(s) Representative at the number below.

If there is a fee occasioned by this response, including an extension fee, that is not covered by an enclosed check, please charge any deficiency to Deposit Account No. 50-3735.

-26-

If the enclosed papers or fees are considered incomplete, the Patent Office is respectfully requested to contact the undersigned Attorney at (508) 616-9660, in Westborough, Massachusetts.

Respectfully submitted,



Paul P. Kriz, Esq.
Attorney for Applicant(s)
Registration No.: 45,752
Chapin Intellectual Property Law, LLC
Westborough Office Park
1700 West Park Drive
Westborough, Massachusetts 01581
Telephone: (508) 616-9660
Facsimile: (508) 616-9661
Customer No.: 58408

Attorney Docket No.: SUN03-14(040486)

Dated: February 2, 2006